Chris Banci

CS436

12/1/17

Lab 6 - Wireshark TCP

1. What is the IP address and TCP port number used by the client computer (source) that is transferring the file to gaia.cs.umass.edu?

* IP address = 192.168.1.102
* TCP port = 1161

1. What is the IP address of gaia.cs.umass.edu? On what port number is it sending and receiving TCP segments for this connection?

* IP address = 128.119.245.12
* TCP port = 80

1. What is the IP address and TCP port number used by your client computer (source) to transfer the file to gaia.cs.umass.edu?

* IP address = 102.168.1.102
* Source port = 59977

1. What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu? What is it in the segment that identifies the segment as a SYN segment?

* The sequence number is 0.
* The SYN Flag set to 1 identifies it as a SYN segment

1. What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN? What is the value of the Acknowledgement field in the SYNACK segment? How did gaia.cs.umass.edu determine that value? What is it in the segment that identifies the segment as a SYNACK segment?

* The sequence number = 0
* The ACK field in the SYNACK segment is set to 1.
* The value was determined by incrementing the initial sequence number.
* The ACK and SYN flag set to 1 indicate it being a SYNACK segment.

1. What is the sequence number of the TCP segment containing the HTTP POST command? Note that in order to find the POST command, you’ll need to dig into the packet content field at the bottom of the Wireshark window, looking for a segment with a “POST” within its DATA field.

* The sequence number that contains the HTTP POST command is 1.

1. Consider the TCP segment containing the HTTP POST as the first segment in the TCP connection. What are the sequence numbers of the first six segments in the TCP connection (including the segment containing the HTTP POST)? At what time was each segment sent? When was the ACK for each segment received? Given the difference between when each TCP segment was sent, and when its acknowledgement was received, what is the RTT value for each of the six segments? What is the EstimatedRTT value (see Section 3.5.3, page 239 in text) after the receipt of each ACK? Assume that the value of the EstimatedRTT is equal to the measured RTT for the first segment, and then is computed using the EstimatedRTT equation on page 239 for all subsequent segments.
2. What is the length of each of the first six TCP segments?

* S1 = 565 bytes
* S2 = 1460 bytes
* S3 = 1460 bytes
* S4 = 1460 bytes
* S5 = 1460 bytes
* S6 = 1460 bytes

1. What is the minimum amount of available buffer space advertised at the received for the entire trace? Does the lack of receiver buffer space ever throttle the sender?

* The minimum amount is 5840 bytes.
* No, the lack of receiver buffer space does not throttle the sender.

1. Are there any retransmitted segments in the trace file? What did you check for (in the trace) in order to answer this question?

* No, there aren't any retransmitted segments
* The sequence numbers were checked to find any retransmitted segments.

1. How much data does the receiver typically acknowledge in an ACK? Can you identify cases where the receiver is ACKing every other received segment (see Table 3.2 on page 247 in the text).

* 1460 bytes of data is typically acknowledged by the receiver in an ACK.
* Segment #80 is a case where the receiver is ACKing every other received segment.

1. What is the throughput (bytes transferred per unit time) for the TCP connection? Explain how you calculated this value.

* The throughput for the TCP connection can be calculated by formula:

throughput = (total data transmitted) / (total transmission time)

* + 30.22 kb/s = (164090) / (5.43)

1. Use the Time-Sequence-Graph(Stevens) plotting tool to view the sequence number versus time plot of segments being sent from the client to the gaia.cs.umass.edu server. Can you identify where TCP’s slowstart phase begins and ends, and where congestion avoidance takes over? Comment on ways in which the measured data differs from the idealized behavior of TCP that we’ve studied in the text.

* The tcp slowstart phase begins at the start of the connection.
* The tcp slowstart phase end and congestion avoidance phase cannot be determined from the graph as it the tcp sender is not sending aggressively enough.

1. Answer each of two questions above for the trace that you have gathered when you transferred a file from your computer to gaia.cs.umass.edu

* The tcp slowstart phase begins at the start of the connection.
* The tcp slowstart phase end and congestion avoidance phase cannot be determined from the graph as it the tcp sender is not sending aggressively enough.